Mandatory Reference: 545, 552
File Name: 545mac_070302_cd28
Revision: 07/03/2002
Effective date: 06/28/2002

Information Technology Security Roles and Responsibilities

Law and Federal guidance require agencies to incorporate security into their information technology architectures and the life cycles of their information systems. More detailed security responsibilities apply to Mission Critical Systems and National Security Systems (see ADS 545, section 545.6, Definitions, for statutory and regulatory terms that apply to information systems).

The Administrator of the United States Agency for International Development (USAID) is the Agency's senior official. In this capacity the Administrator is responsible for developing and implementing a comprehensive, Agency-wide information systems (IS) security program that is technically current, cost effective, and in full compliance with established national security directives. This responsibility has been delegated to the Bureau for Management, Office of Information Resources Management (M/IRM).

Managers, Bureau Chiefs, Directors, designated Information Systems Security Officers (ISSOs) (both the ISSO for USAID and ISSOs within USAID organizational units), Information Technology (IT) Specialists (USAID/W), System Managers (USAID Missions), IT system staff, and users also have important IS security roles and responsibilities. For more details on USAID's official delegations of authority, see ADS 103, Delegations of Authority. Mandatory USAID information technology (IT) security roles and responsibilities follow.

NOTE: More details on Agency Incident Response responsibilities are contained in the Internal Mandatory Reference, "Incident Response Guidance for Unclassified Information Systems." Details on Certification and Accreditation responsibilities are contained in the Internal Mandatory Reference, "Information Systems Certification and Accreditation Process, Approval to Operate."

1. The Assistant Administrator, Bureau for Management (AA/M) serves as the Agency's Chief Information Officer (CIO), and is responsible for directing, managing, and providing policy guidance and oversight with respect to all Agency information resource management activities. These responsibilities may be delegated to senior-level office managers. The CIO serves as the Designated Security Accreditation Authority (DSAA) for most of USAID's IS, including IS at USAID Missions.

2. The Director, Office of Financial Management (M/FM), serves as the DSAA for financial IS in USAID/Washington (USAID/W).

3. The Bureau for Management, Office of Information Resources Management (M/IRM) is responsible for providing "signatory approval to operate" for all information systems used to process, store, or print Sensitive But Unclassified information. The Director of M/IRM has the authority to approve, subsequent to coordination with the Director of the Office of Security (D/SEC), the use of all information systems used to process, store, or print classified national security information. The Director of M/IRM has been assigned responsibility for management and oversight of Agency information system resource programs, and for compliance with Federal regulations related to paperwork reduction, TEMPEST, Communications Security (COMSEC), and operational security for secure telephone units.

4. The ISSO for USAID is designated by the Administrator to oversee and direct the implementation and operation of the Agency's Information Systems Security (ISS) program across all Offices, Bureaus, and Missions. The USAID ISSO has been specifically tasked to monitor Information Systems (IS) and to render assistance in the investigation of computer crimes and incidents that affect the Agency. In addition, the ISSO is authorized to coordinate infrastructure assurance activities with other Federal departments and agencies. USAID’s ISSO is directly responsible for the following:

a. Reporting on all Agency information systems security issues to the Director of M/IRM;

b. Reviewing and coordinating all requests for exemptions to the Agency's information systems security policy as explained in ADS chapters 545 and 552;

*c. Directing inquiries into suspected security incidents involving system assets (see note below and Mandatory Reference, “Incident Response Guidance for Unclassified Information Systems”);

d. Coordinating investigations, with the Office of Security, of all suspected computer security violations, incidents, and compromises of classified national security information;

e. Coordinating and/or participating in actions taken as a result of suspected or proven security incidents involving information systems;

f. Serving as the primary point of contact for information systems security issues and inquiries for designated ISSOs throughout the Agency;

g. Providing the information technology security interface between M/IRM divisions and other Agency organizations;

h. Reviewing and approving all encryption methodologies (including hardware, software, and encryption logarithms) proposed for USAID equipment, systems, networks, or enterprise architectures; and

i. Representing the Agency in intergovernmental and interagency organizations and specialized groups at the working group level.

NOTE: Government Information Security Reform legislation and regulatory guidance stress the importance of incident response to protecting IS. Given the highly networked nature of the Federal computing environment, all agencies must implement improved security management measures, to assure that opportunities for interoperability are not adversely affected by inadequate security controls. Should an incident occur, a prompt, coordinated response can limit damage, speed recovery, and help restore service to users. USAID's ISSO, after consultation with the Office of Security (SEC), will develop and implement methodologies for

- Detecting, reporting, and responding to IS security incidents;

- Notifying the Office of Inspector General about IS security incidents involving any apparent violation of laws, rules, or regulations; and

- Notifying and consulting with other offices and authorities, to include the General Services Administration's Federal Computer Incident Response Capability (FedCIRC), in the event that a significant IS security incident occurs.

5. The Office of Inspector General (OIG), consistent with legal and regulatory guidance, will conduct evaluations of USAID IS.

6. The Bureau for Management, Office of Information Resources Management, Telecommunications and Computer Operations Division (M/IRM/TCO) is directly responsible for ensuring that each Agency facility is supported by telecommunications and computer resources capable of operating in compliance with the Agency's information systems security program and policy.

7. The Bureau for Management, Office of Information Resources Management, Systems Development and Maintenance Division (M/IRM/SDM) is directly responsible for the following:

a. Ensuring that corporate application software and system maintenance resources are capable of operating in compliance with the Agency's information systems security program policy; and

b. Ensuring that operational and functional software security controls are provided for the technical enforcement of need-to-know restrictions on all information systems equipment operating in a distributed or network mode.

8. The Bureau for Management, Office of Information Resources Management (M/IRM) and the ISSO for USAID are jointly and directly responsible for the following:

a. Addressing computer and communications security issues during system migration planning, system architecture planning, information engineering, and new system technology research and development;

b. Incorporating computer and communications security as an evaluation element in the overall Agency information management (IM) quality assurance program;

c. Coordinating the development of contract security classification specifications (DD Form 254 or equivalent) for maintenance and service contracts supporting Sensitive But Unclassified (SBU) and classified information systems with the Office of Security (SEC) and the Office of Procurement (M/OP) – see also ADS 567, Classified Contracts, Grants, and Cooperative Agreements, and Contractor/Recipient Personnel Security;

d. Developing and implementing the Agency's information systems security program;

e. Assisting in the accomplishment of risk, sensitivity, or vulnerability assessments in support of systems life-cycle activities or continuing Agency risk management, and coordinating, when appropriate, the resulting reports at or above the division chief level;

f. Developing, implementing, and supporting an Agency-wide information systems security awareness and education program;

g. Ordering and coordinating the installation of secure telephone units (STU-III) in Agency facilities with the Department of State COMSEC Accountant; and

h. Maintaining COMSEC accountability, keeping an up-to-date inventory of STU-III systems and other controlled cryptographic items, as well as instituting a cryptographic key management procedure.

9. Information Technology (IT) Specialists (USAID/W), System Managers (USAID Missions), and system staff are directly responsible for the following:

a. Ensuring that all the information systems they manage are operated, on a day-to-day basis, in compliance with the Agency's information systems security policy and guidelines;

b. Coordinating with the system staff implementation of information systems security standards for information systems;

c. Providing the designated ISSO with technical support and expertise in the implementation of Agency information systems security policies;

d. Maintaining an inventory of all hardware, operating system software, application software, peripheral devices, and communication links that are part of the system(s) they manage, and reporting all incidents of lost or stolen equipment to the appropriate security office; and

*e. [Moved from former section 12.b] Informing the designated ISSO of any security incidents related to software applications supporting their program or system users; and

f. Disseminating the Agency's system security policies, procedures, and guidelines to all users of the system(s) they manage.

10. The COMSEC Custodian and Alternate are cleared, U.S. citizen, direct-hire employees of the Agency who are designated by either M/IRM (USAID/W) or Mission Directors/Representatives and are directly responsible for the following:

a. Ordering cryptographic keys;

b. Managing keying material and STU-III equipment accounting services in accordance with mandatory procedures delineated in NTISSI No. 4001 /CSISM/CCI and other applicable national-level guidance;

c. Ensuring facility/Mission compliance with national and Agency communication policy;

d. Assisting the ISSO for USAID in maintaining COMSEC accountability, keeping an up-to-date inventory of STU-III systems, and instituting a cryptographic key management procedure; and

e. Coordinating investigations of lost or suspected loss of COMSEC or cryptographic equipment and materials with the Office of Security (SEC).

11. A statement specifying responsibilities for information systems security must be included in position descriptions and work requirements statements for IT Specialists /System Managers and members of the system staff having responsibility for programming, operating, or managing applications or systems. The Bureau for Management, Office of Human Resources (M/HR) is available to assist USAID supervisors in developing position descriptions.

*12. Program Managers and Mission Directors have management responsibilities for USAID IS used to execute their operations. Program Managers may either serve as Certification Authorities themselves, or may elect to have a designated ISSO serve as the Certification Authority, for major applications or support systems under their control. Mission Directors at USAID Missions serve as Certification Authorities, and certify IS that support operations conducted in their organizations. Program Managers and Mission Directors are directly responsible for the following:

a. Determining which system users have a verifiable need to access applications, programs, and sub-programs used to support their job tasks and responsibilities, and informing the IT Specialist/System Manager, in writing, of all system access requirements;

*[former section 12.b moved to 9.e]

b. Appointing in writing U.S. citizens with at least Secret security clearances as designated ISSOs and alternates to implement the Agency's information systems security policies and guidelines for their programs and Missions. The designated ISSO at USAID Missions is usually the Executive Officer (EXO); however, a Mission Director may appoint another U.S. citizen with at least a Secret clearance as designated ISSO instead; and

c. Managing the overall information systems security program for their functional areas, including the implementation of all applicable information systems security policies and guidelines as described in ADS 545.

13. The designated ISSO and alternate are appointed by the Program Manager or the IT Specialist's first-line supervisor at USAID/W. The designated ISSO is responsible for the following:

a. Implementing Agency information systems security policy and guidelines as directed in ADS 545 and as it applies to information systems managed by the designated ISSO;

b. Keeping the Mission Director/Representative, System Manager, ISSO for USAID, and other facility security personnel apprised of all suspected or known security incidents, violations, and/or compromises associated with the information system(s) managed by the ISSO;

c. Providing technical assistance during system security investigations conducted by authorized Agency personnel or bona fide representatives;

d. Conducting basic security awareness training for end-user personnel authorized to access the information system(s) managed by the ISSO;

e. Conducting annual self-evaluation reviews of the information systems security program managed by the designated ISSO;

f. Coordinating with the Department of State's embassy or consulate ISSO, Regional Security Officer, and/or Security Engineering Officer on all issues associated with automation security; and

*g. Providing input for the development of a security plan for the Mission General Support System and MACS (if present). An on-line survey tool is provided for this purpose at **http://inside.usaid.gov/M/IRM/ipa/iss/progmgmt/secplan/main.htm**. Designated ISSOs and System Managers/IT Specialists must use this tool to provide data for development of an initial security plan. If a Mission or site does not have access to the USAID intranet or requires samples, contact rmurphy@usaid.gov.

14. Users of USAID information systems are directly responsible for the following:

a. Abiding by Agency information systems security polices and guidelines as directed in the ADS 500 series; and

b. Reporting system or application irregularities or suspected security violations to the Program Manager, Mission Director/Representative, designated ISSO, or System Manager/Administrator.

15. The Director, Office of Security is responsible for the following:

a. Coordinating with the ISSO for USAID the reporting and investigation of suspected or known IS security incidents, violations, and compromises, including those involving COMSEC and cryptographic equipment and materials;

b. Performing inspections of USAID information systems to ensure that classified national security information is properly protected;

c. Conducting background checks on all U.S. citizens requesting access to USAID systems that process, store, or control sensitive information (See ADS 566 and ADS 567); and

d. Approving, in coordination with the Director, M/IRM, the authority of overseas Missions and USAID/Washington Bureaus/Independent Offices to process classified national security information on an information technology system.